FB.WS\_WRITEOBJECT\_SYNC

Этот класс имеет метод writeObject(), который синхронизируется; однако ни один другой метод класса не синхронизируется.

Таблица №1 – Основные характеристики детектора FB.WS\_WRITEOBJECT\_SYNC

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Serialization Vulnerability |
| CWE | --- |
| CVE | --- |
| Возможные последствия | Deadlock при сериализации объекта; снижение производительности из-за блокировок; потенциальная потеря данных при конкурентном доступе |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() {  class SyncSerializable implements Serializable {  private final Object lock = new Object();  private int value;  private void writeObject(ObjectOutputStream out) throws IOException {  synchronized (lock) { // Опасная синхронизация при сериализации  out.defaultWriteObject();  }  }  }  SyncSerializable obj = new SyncSerializable();  try (ByteArrayOutputStream bos = new ByteArrayOutputStream();  ObjectOutputStream oos = new ObjectOutputStream(bos)) {  oos.writeObject(obj);  } catch (IOException e) {  e.printStackTrace();  }  } | public static void correctTest() {  class SafeSerializable implements Serializable {  private transient final Object lock = new Object(); // transient для несериализуемого поля  private int value;  private void writeObject(ObjectOutputStream out) throws IOException {  out.defaultWriteObject(); // Без синхронизации  }  }  SafeSerializable obj = new SafeSerializable();  try (ByteArrayOutputStream bos = new ByteArrayOutputStream();  ObjectOutputStream oos = new ObjectOutputStream(bos)) {  oos.writeObject(obj);  } catch (IOException e) {  e.printStackTrace();  }  } |